

GAO

Accounting and Information  
Management Division

---

August 1999

# Information Security Risk Assessment

Practices of Leading  
Organizations

**Exposure Draft**

## Form SF298 Citation Data

<b>Report Date</b> <i>("DD MON YYYY")</i> 01081999	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> <i>("DD MON YYYY")</i>
<b>Title and Subtitle</b> Information Security Risk Assessment: Practices of Leading Organizations. Exposure Draft		<b>Contract or Grant Number</b>
		<b>Program Element Number</b>
<b>Authors</b>		<b>Project Number</b>
		<b>Task Number</b>
		<b>Work Unit Number</b>
<b>Performing Organization Name(s) and Address(es)</b> GAO		<b>Performing Organization Number(s)</b>
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>		<b>Monitoring Agency Acronym</b>
		<b>Monitoring Agency Report Number(s)</b>
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b>		
<b>Abstract</b>		
<b>Subject Terms</b> "IATAC COLLECTION"		
<b>Document Classification</b> unclassified		<b>Classification of SF298</b> unclassified
<b>Classification of Abstract</b> unclassified		<b>Limitation of Abstract</b> unlimited
<b>Number of Pages</b> 53		

<b>REPORT DOCUMENTATION PAGE</b>			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> 8/1/99	<b>3. REPORT TYPE AND DATES COVERED</b> Report	
<b>4. TITLE AND SUBTITLE</b> Information Security Risk Assessment: Practices of Leading Organizations (GAO/AIMD-99-139)			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> GAO				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b>				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b>			<b>12b. DISTRIBUTION CODE</b>  A	
<b>13. ABSTRACT (Maximum 200 Words)</b> This guide, which we are initially issuing as an exposure draft, is intended to help federal managers implement an ongoing information security risk assessment process by providing examples, or case studies, of practical risk assessment procedures that have been successfully adopted by four organizations known for their efforts to implement good risk assessment practices. More importantly, it identifies, based on the case studies, factors that are important to the success of any risk assessment program, regardless of the specific methodology employed.				
<b>14. SUBJECT TERMS</b> Information, Security, Risk			<b>15. NUMBER OF PAGES</b>	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> UNCLASSIFIED	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> UNCLASSIFIED	<b>20. LIMITATION OF ABSTRACT</b>  None	

## Preface

Managing the security risks associated with our government's growing reliance on information technology is a continuing challenge. In particular, federal agencies, like many private organizations, have struggled to find efficient ways to ensure that they fully understand the information security risks affecting their operations and implement appropriate controls to mitigate these risks.

This guide, which we are initially issuing as an exposure draft, is intended to help federal managers implement an ongoing information security risk assessment process by providing examples, or case studies, of practical risk assessment procedures that have been successfully adopted by four organizations known for their efforts to implement good risk assessment practices. More importantly, it identifies, based on the case studies, factors that are important to the success of any risk assessment program, regardless of the specific methodology employed.

The information provided in this document supplements guidance provided in our May 1998 executive guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). In that guide, we outlined five major elements of risk management and 16 related information security management practices that GAO identified during a study of organizations with superior information security programs. One of the five elements identified encompasses assessing risk and determining risk-reduction needs. Contributors to this supplementary guide include Jean Boltz, Ernest Döring, and Michael Gilmore.

You may submit comments before September 30, 1999, by phone, e-mail, or regular mail to Jean Boltz at the following:

Phone: (202) 512-5247

E-mail: [boltzj.aimd@gao.gov](mailto:boltzj.aimd@gao.gov)

Mail: Jean Boltz, AIMD  
U.S. General Accounting Office  
Room 4T21  
441 G Street, NW  
Washington, D.C. 20548

Jack L. Brock, Jr.  
Director, Governmentwide and Defense  
Information Systems

# Contents

<b>Introduction</b>	<b>5</b>
Federal Guidance	5
Risk Assessment Is an Essential Element of Risk Management	6
Basic Elements of the Risk Assessment Process	7
Challenges Associated With Assessing Information Security Risks	8
<b>Overview of Case Study Findings</b>	<b>10</b>
Critical Success Factors	12
Tools	16
Benefits	17
<b>Case Study 1: Multinational Oil Company</b>	<b>19</b>
Distinguishing Characteristics	19
Initiating a Risk Assessment	21
Conducting and Documenting the Assessment	21
Reporting and Ensuring that Agreed Upon Actions are Taken	25
<b>Case Study 2: Financial Services Company</b>	<b>27</b>
Distinguishing Characteristics	27
Initiating a Risk Assessment	29
Conducting and Documenting the Assessment	29
<b>Case Study 3: Regulatory Organization</b>	<b>35</b>
Distinguishing Characteristics	35
Initiating a Risk Assessment	37
Conducting and Documenting the Assessment	37
Reporting and Ensuring that Agreed Upon Actions are Taken	41

<b>Case Study 4: Computer Hardware and Software Company</b>	<b>42</b>
---	-----------

Distinguishing Characteristics	42
Initiating a Risk Assessment	44
Conducting and Documenting the Assessment	44
Reporting and Ensuring that Agreed Upon Actions are Taken	49

---

<b>Appendix I - Objectives and Methodology</b>	<b>50</b>
--	-----------

---

<b>Tables</b>	
---------------	--

Table 1: Risk Assessment Matrix	39
Table 2: Risk Assessment Table	40

---

<b>Figures</b>	
----------------	--

Figure 1: Risk Management Cycle	7
Figure 2: Risk Assessment Practices and Related Benefits	11
Figure 3: Risk Assessment Process Diagram 1	20
Figure 4: Risk Assessment Matrix	25
Figure 5: Risk Assessment Process Diagram 2	28
Figure 6: Abbreviated Example of Standardized Questionnaire	31
Figure 7: Risk Assessment Process Diagram 3	36
Figure 8: Elements Considered in Ranking Risk	38
Figure 9: Risk Assessment Process Diagram 4	43
Figure 10: Questionnaire Items Related to Authorization	46
Figure 11: Example of Five Strength Levels for Security Training	48

---

<b>Abbreviations</b>	
----------------------	--

GAO	General Accounting Office
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

## Introduction

The federal government is increasingly reliant on automated and interconnected systems to perform functions essential to the national welfare, such as national defense, federal payments, and tax collection. The benefits of such activities include improved government information processing and communication. However, the factors that benefit government operations—speed of processing and access to information—also increase the risks of computer intrusion, fraud, and disruption.

Information systems have long been at some risk from malicious actions or inadvertent user errors and from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or “hacking,” techniques are becoming more widely known via the Internet and other media.

Numerous government reports published over the last few years indicate that federal automated operations and electronic data are inadequately protected against these risks. These reports show that poor security program management is one of the major underlying problems. A principal challenge many agencies face is in identifying and ranking the information security risks to their operations, which is the first step in developing and managing an effective security program. Taking this step helps ensure that organizations identify the most significant risks and determine what actions are appropriate to mitigate them.

## Federal Guidance

The Office of Management and Budget (OMB), as part of Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” requires federal agencies to consider risk when deciding what security controls to implement. It states that a risk-based approach is required to determine adequate security, and it encourages agencies to consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. The OMB Director reiterated these responsibilities on June 23, 1999, when he issued Memorandum 99-20, “Security of Federal Automated Information Resources,” reminding federal agencies that they must continually assess the risk to their computer systems and maintain adequate security commensurate with that risk. This memorandum was issued in response to a spate of intentional disruptions of government web sites.



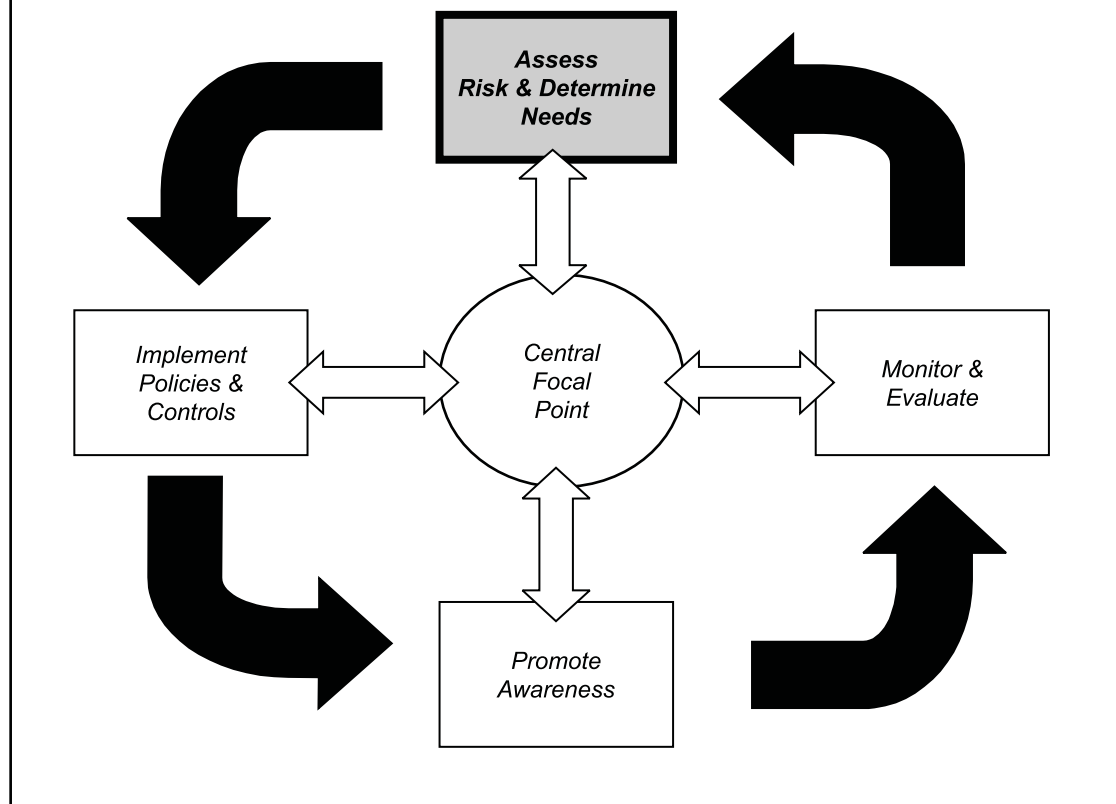
The National Institute of Standards and Technology (NIST) also recognizes the importance of conducting risk assessments for securing computer-based resources. NIST's guidance on risk assessment is contained in An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, December 1995, and Generally Accepted Principles and Practices for Securing Information Technology Systems, published in September 1996.

## **Risk Assessment Is an Essential Element of Risk Management**

As discussed in our May 1998 executive guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), assessing risk is one element of a broader set of risk management activities. Other elements include establishing a central management focal point, implementing appropriate policies and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness.

Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. This continuing cycle of activity, including risk assessment, is illustrated in the following depiction of the risk management cycle.

**Figure 1: Risk Management Cycle**



## Basic Elements of the Risk Assessment Process

Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decisionmakers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. For example, bank officials have conducted risk assessments to manage the risk of default associated with their loan portfolios, and nuclear power plant engineers have conducted such assessments to manage risks to public health and safety. As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being considered, all risk assessments generally include the following elements.

- Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.

- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.
- Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
- Documenting the results and developing an action plan.

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on (1) the likelihood that a damaging event will occur, (2) the costs of potential losses, and (3) the costs of mitigating actions that could be taken. When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low. In this regard, qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

## **Challenges Associated With Assessing Information Security Risks**

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing. For example,

- data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses;

- some costs, such as loss of customer confidence or disclosure of sensitive information, are inherently difficult to quantify;
- although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented; and
- even if precise information were available, it would soon be out of date due to fast-paced changes in technology and factors such as improvements in tools available to would-be intruders.

This lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which controls are the most cost-effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.

To assist agencies in meeting this challenge and to supplement our May 1998 guide on information security management, we studied the practices of four organizations that had institutionalized practical risk assessment methods. We identified these organizations based on recommendations from government and private sector sources. These sources recommended over 30 private and public sector organizations that were known to have strong security programs or be actively pursuing improved risk assessment practices. The four organizations included a multinational oil company, a financial services company, a regulatory organization, and a computer hardware and software company. This guide describes the factors that these organizations considered critical to the success of their risk assessment processes and the benefits they cited as a result of these practices. In addition, it provides a description of the procedures they followed and examples of the tools they used to facilitate the process.

The organizations we selected had chosen risk assessment methods and developed tools that were relatively simple and, for the most part, qualitative in nature. However, one organization used a combination of qualitative and quantitative methods. In some cases, agencies may find that it is more appropriate to use more detailed, quantitative methods to assess the risks associated with certain aspects of their computerized operations. However, incorporating the critical success factors that we identified is likely to make any type of methodology more effective. Appendix I contains a more detailed description of the scope of our study and the methodology we used.

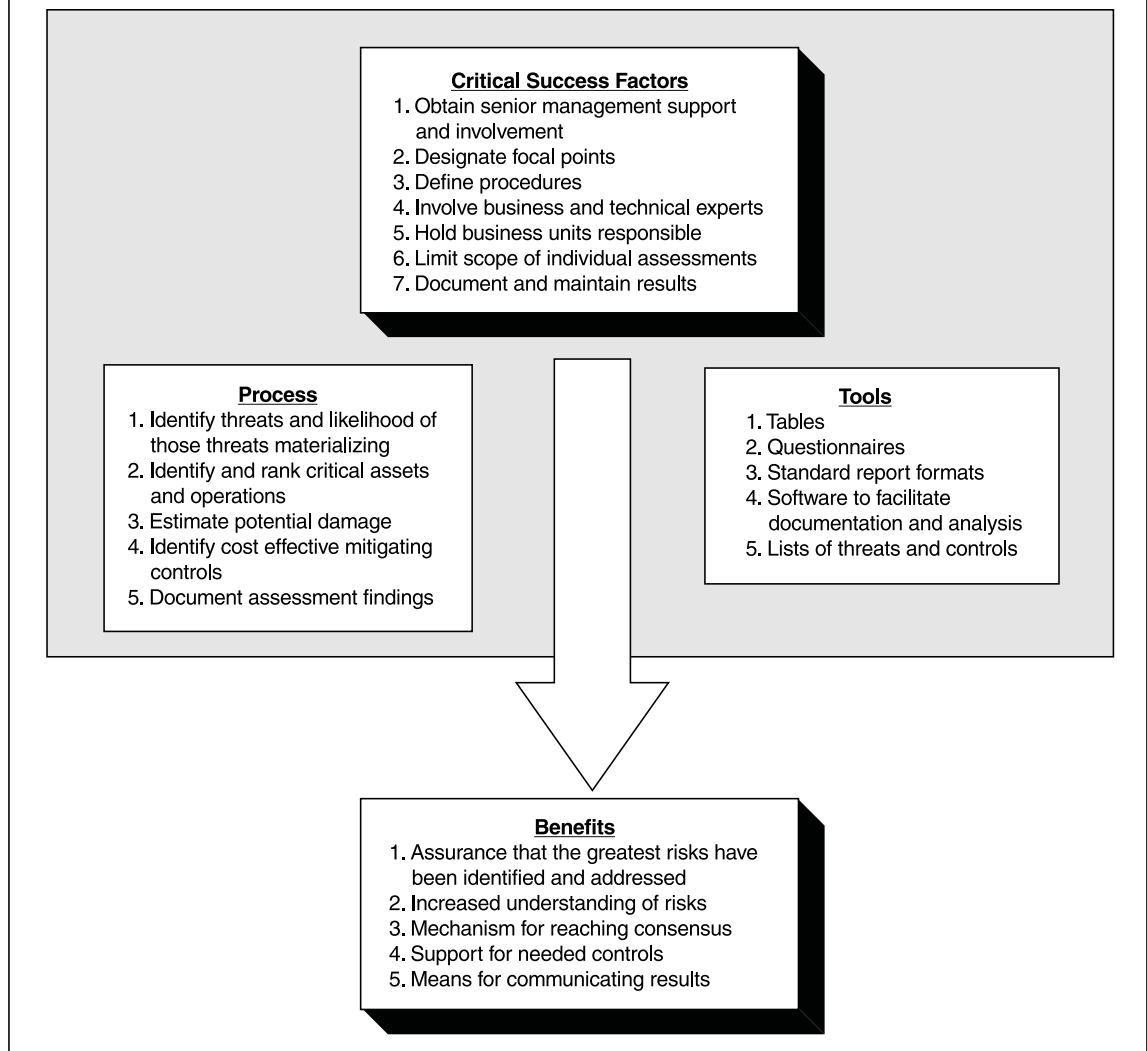
## Overview of Case Study Findings

The organizations in our study recognized that risk assessments were an integral part of managing risks. They had developed various procedures and tools to ensure that this aspect of their information security programs was not neglected. They also recognized that the data on threat likelihood and on the costs of risk reduction techniques were limited, but they did not believe these limitations precluded effectively exploring, understanding, and ranking information security risks to their operations and assets. The procedures they had implemented helped ensure that these risks were periodically discussed and understood and that the most significant risks were identified and addressed. In their view, achieving these benefits far outweighed the costs of performing the risk assessment procedures they had adopted.

Although all of the organizations had long considered various risks to their business operations, their increased reliance on networked computer systems in recent years had accentuated serious and real vulnerabilities and prompted them to bolster their efforts to assess information security risks. All had begun to improve and better define their information security risk assessment processes during the previous 2 to 4 years, and all were continuing to refine the process as they gained experience.

Although their methods and tools varied, the organizations cited similar practices that they considered to be essential to the success of their risk assessment programs. They also cited similar benefits, such as increased understanding of risks and support for needed controls throughout the organization. The critical success factors, methods and tools, and benefits are illustrated in the following diagram.

**Figure 2: Relationship of Risk Assessment Practices in Achieving Benefits**



## **Critical Success Factors**

During our study, we identified a set of common critical success factors that were important to the efficient and effective implementation of the organizations' information security risk assessment programs. These factors helped ensure that the organizations benefited fully from the expertise and experience of their senior managers and staff, that risk assessments were conducted efficiently, and that the assessment results led to appropriate remedial actions. As might be expected, several of these factors are similar to the more general information security management practices identified in our May 1998 executive guide.

### **Obtain Senior Management Support and Involvement**

Senior management support was important to ensure that risk assessments were taken seriously at lower organizational levels, that resources were available to implement the program, and that assessment findings resulted in implementation of appropriate changes to policies and controls. This support extended to participating in key aspects of the process, such as (1) assisting in determining the assessment's scope and the participants at the start of a new assessment and (2) approving the action plan developed to respond to recommendations at the end. For example, at the oil company we studied, business units were keenly aware of the importance of conducting risk assessments due largely to the expectations of senior executives and the related support they provided. Security was paramount in this organization and failure to comply with organizational risk assessment policy required significant justification on the part of the business owner. Also, senior managers at the unit being assessed were actively involved in determining the scope of each assessment and in responding to final results and recommendations.

### **Designate Focal Points**

Groups or individuals had been designated as focal points to oversee and guide the organizations' risk assessment processes. These focal points facilitated the planning, performance, and reporting associated with the organizations' risk assessment programs and helped ensure that organizationwide issues were appropriately addressed. All focal points were either located at the corporate level or were members of a corporate-level committee that coordinated the progress of the risk assessment from an organizationwide viewpoint.

- At the oil company, a corporate-level facilitator served as a focal point for assessments throughout the company, including those pertaining to information security. Because of familiarity with the tools and the reporting requirements, this

experienced individual helped reduce the amount of training required for others involved in the process, such as those responsible for collecting and analyzing data.

- At the financial services company, each business unit had a designated individual responsible for the business unit's risk assessment activities. The facilitators generally met weekly as a group to discuss organizationwide risks and lessons learned from prior and ongoing assessments.
- At the computer hardware and software company, a council had been created for the purpose of improving the overall risk assessment process and reviewing the results of risk assessments.

In addition, corporate focal points were involved in developing, disseminating, and periodically updating risk assessment guidance and often provided training to others.

The use of focal points enhanced the quality and efficiency of the risk assessments. In particular, using focal points to coordinate the planning and performance of the risk assessments helped ensure that

- tools were used effectively under the direction of an individual who was experienced in using them,
- successful techniques were promptly applied to subsequent assessments,
- terms and methods were applied consistently,
- reports were developed quickly and according to a standardized format, and
- expectations of senior executives were met.

## **Define Procedures**

Each organization had defined and documented procedures for conducting risk assessments and developed tools to facilitate and standardize the process. These, along with the use of focal points, helped institutionalize the process, ensure a level of assessment consistency, and prevent individual business units from “reinventing the wheel” each time a new assessment was required. To provide flexibility, business units generally could supplement or alter procedures when needed. These modifications were often shared with other units in an effort to promote the use of best practices.

Defined procedures generally specified

- who was responsible for initiating and conducting risk assessments,
- who was to participate,
- what steps were to be followed,
- how disagreements were to be resolved,
- what approvals were needed,
- how assessments were to be documented,



- how documentation was to be maintained, and
- to whom reports were to be provided.

### **Involve Business and Technical Experts**

Drawing on knowledge and expertise from a wide range of sources was viewed as essential to help ensure that all important risk factors were considered. Business managers generally had the best understanding of the criticality and sensitivity of individual business operations and of the systems and data that supported these operations. Accordingly, they were usually in the best position to gauge the business impact of system misuse or disruption. Conversely, technical personnel, including security specialists, brought to the process an understanding of existing system designs and vulnerabilities and of the potential benefits, costs, and performance impacts associated with new controls being considered. As a result, meetings conducted during the risk assessment process usually included a variety of individuals from the business unit with expertise in business operations and processes, security, information resource management, information technology, and system operations. Others from outside the business unit might also be included, such as internal auditors and, occasionally, contractors with specific pertinent expertise.

All the organizations relied almost exclusively on in-house personnel to perform the risk assessment rather than contractors. The computer hardware and software company initially relied on contractors to assist in conducting assessments but eventually determined that relying on contractors deprived its own personnel of valuable experience in exploring risk.

The oil company had established a special unit to gather information on threats from outside sources, including federal agencies and organizations such as Carnegie Mellon University's Computer Emergency Response Team Coordination Center. This helped ensure that the organization fully understood the threats that might affect its worldwide operations and that risk assessment teams considered this information in their analyses. Similarly, the financial services company required individuals with expertise in specific geographic areas to provide input on pertinent political and economic risk factors.

### **Hold Business Units Responsible**

Responsibility for initiating and conducting risk assessments, as well as following up on resulting recommendations, lay primarily with the individual business units. Business units were considered to be in the best position to determine when an assessment was needed and to ensure that recommendations for risk reduction techniques resulting from the assessment were implemented effectively.

- At the financial services company, the business units annually developed risk management plans from a variety of information sources, including the results of prior risk assessments. These plans served as a basis for establishing priorities for performing risk assessments; designating individuals to facilitate, coordinate, and execute risk assessment activities; and determining the tolerable level of risk for a given operation.
- At the computer hardware and software company, business unit managers were responsible for assessing the risks associated with their unit's computer-based operations, and such responsibilities were generally documented in their performance expectations.
- At the oil company, the business unit was responsible for initiating a risk assessment and approving an assessment execution plan. This plan, initially drafted by a headquarters-level facilitator, included the assessment scope, list of questions to be addressed during the process, and list of individuals that would participate in the assessment.

### **Limit Scope of Individual Assessments**

Rather than conducting one large risk assessment covering all of an entity's operations at once, the organizations generally conducted a series of narrower assessments on various individual segments of the business. As a result, the scope of each assessment was limited to a particular business unit, system, or facility, or to a logically related set of operations.

Segmenting operations into logical units generally reduced the size of each assessment, making it more manageable to schedule and perform. In addition, segmenting operations provided organizations a means of ranking units to determine the order in which risk assessments would be performed and which units might merit more frequent risk assessments.

- A regional office at the regulatory organization decided that, after reviewing its processes, it would do two separate risk assessments—one on its administrative operations and one on its business-related operations. Managers decided to separate the assessments because the two sets of operations relied on different systems and were subject to somewhat different risks.
- At the computer hardware and software company, risk assessment scope was generally focused on each primary business process and its supporting systems, including the software, databases, and the hardware and network technology supporting the software.

To successfully implement this unit-by-unit approach, provisions had to be made for considering shared risks and risks associated with infrastructure systems, such as electronic mail systems and other shared resources, which supported multiple units of the organization.

- The regulatory organization centrally evaluated the controls associated with its organizationwide electronic mail system and determined that the controls over this system were adequate to support low- and medium-risk applications. Individual units subsequently used this information to determine the extent to which specific business operations should rely on the electronic mail system.
- At the financial services company, a corporate-level group of risk assessment focal points met twice weekly to consider corporatwide risks and approve actions at individual units that might affect the entire organization.

## **Document and Maintain Results**

Risk assessment results were documented and maintained so that managers could be held accountable for the decisions made and a permanent record established. In this way, risk assessment records were available to serve as the starting point for subsequent risk assessments and as a ready source of useful information for managers new to the business unit. Documenting the process undertaken also permitted others, such as the internal audit department, to ensure that organizational units were complying with company policy.

All the organizations maintained databases on the results of the assessments. These results were used as the starting point for subsequent risk assessments and to monitor the status of any open recommendations for mitigating risks identified during the process. For example, at the financial services company, the documentation created during a risk assessment was used as the basis for the following year's risk management plan. At the regulatory organization, an internally developed software program was used to monitor the implementation status of assessment recommendations and to report the status to senior management.

## **Tools**

All of the organizations we studied had developed tools to facilitate the conduct of their risk assessments, such as tables, questionnaires, and standard report formats. These tools helped ensure a consistent and standardized approach throughout the organization and prevented teams from "reinventing the wheel" each time a new assessment was initiated.

Such tools had been developed in-house or adapted from those used by others, and most had been computerized to speed the documentation process and to provide easy access to data and risk assessment results. Generally, the corporate offices responsible for overseeing risk assessment activities periodically refined the tools as experience was gained and best practices were identified.

Most of these tools were relatively simple aids to assessment and reporting, although one organization had automated the majority of its analysis process.

- The oil company used a table, in the form of a matrix, that facilitated analysis of information security risks to its operations and served as an effective tool for communicating risk assessment results to management. The matrix showed the combined effects of the probability of an undesirable event occurring and the severity of damage or loss to key organizational assets or operations if the event were to occur.
- The financial services company used a questionnaire to document compliance or noncompliance with company control objectives and the specific control techniques employed. The questionnaire was organized by specific control objectives, such as authentication, access control, confidentiality, availability, audit, and administration.
- The computer hardware and software company had developed relatively more sophisticated tools, including a detailed software program that had been designed to draw on large amounts of data on risk factors and automatically analyze input from the risk assessment team.

Tools used by the organizations we studied are described and illustrated in the case study descriptions included in this guide.

## **Benefits**

The organizations in our study told us that institutionalizing a practical risk assessment program was important to supporting their business activities and provided several benefits. First, and perhaps most importantly, risk assessment programs helped ensure that the greatest risks to business operations were identified and addressed on a continuing basis. Such programs helped ensure that the expertise and best judgments of their personnel were tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the organization's mission.

Second, risk assessments helped personnel throughout the organization better understand risks to business operations; avoid risky practices, such as disclosing passwords or other

sensitive information; and be alert for suspicious events. This understanding grew, in part, from improved communication between business managers, system support staff, and security specialists.

Further, risk assessments provided a mechanism for reaching a consensus on which risks were the greatest and what steps were appropriate for mitigating them. The processes used encouraged discussion and generally required that disagreements be resolved. This, in turn, made it more likely that business managers would understand the need for agreed upon controls, feel that the controls were aligned with the unit's business goals, and support their effective implementation. Officials at one organization told us that controls selected in this manner were much more likely to be effectively adopted than controls that had been imposed by personnel outside of the business unit.

Finally, a formal risk assessment program provided an efficient means for communicating assessment findings and recommended actions to business unit managers as well as to senior corporate officials. Standard report formats and the periodic nature of the assessments provided organizations a means of readily understanding reported information and comparing results among units over time.

## **Case Study 1: Multinational Oil Company**

### **Distinguishing Characteristics**

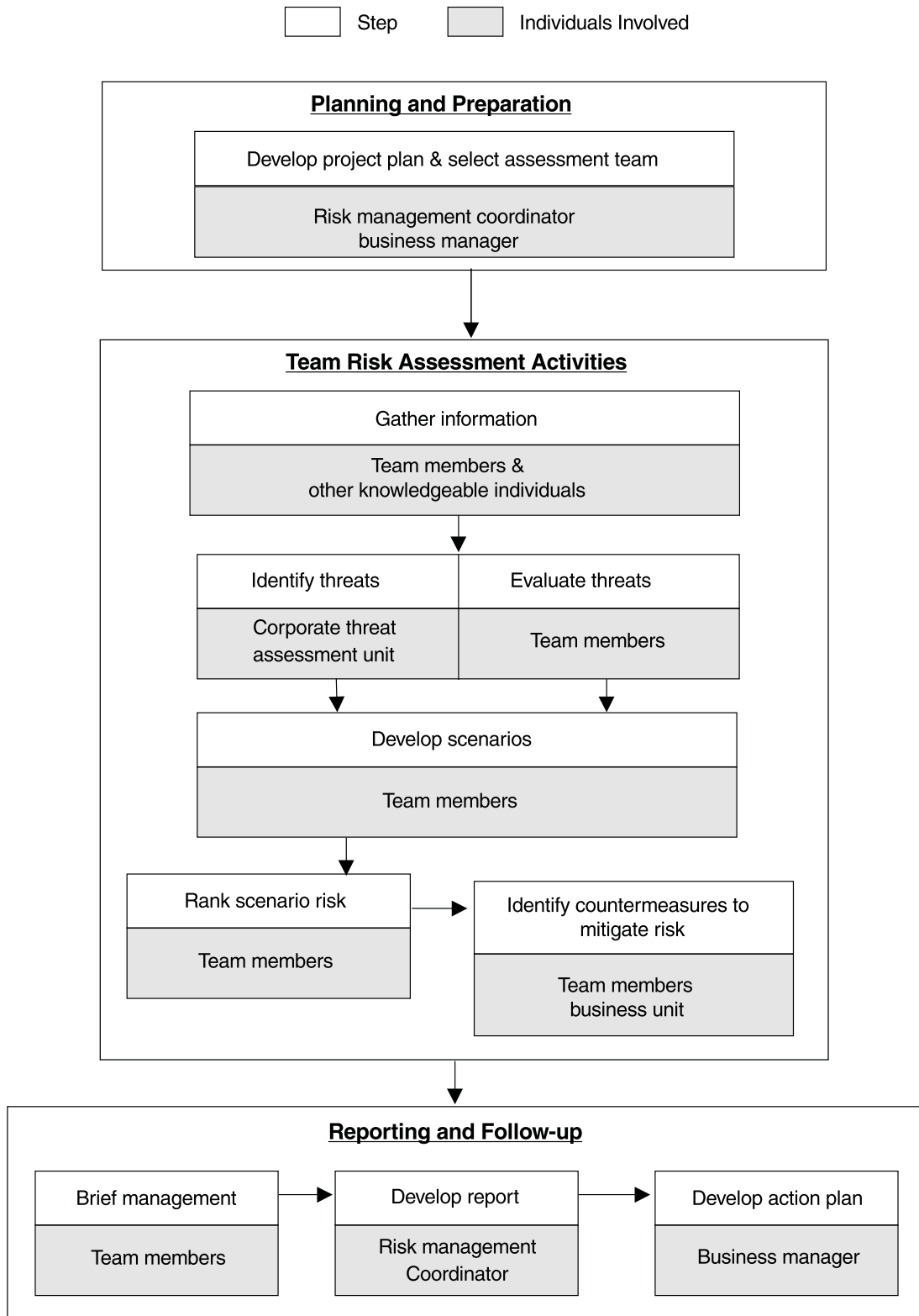
- Established single corporate focal point.
- Focused on specific scenarios.
- Ensured that decisions were consensus-based.
- Built on processes developed by others.

This organization has a wide range of operations in 30 countries with varying levels of risk. Security and safety concerns are critical factors in conducting business, and risk assessments are a key component for addressing those concerns. Failure to comply with organizational risk assessment policy requires significant justification on the part of the business owner. Although risk assessments have been a part of doing business since the mid-1980s, the organization has been striving to implement a more disciplined approach since 1995.

At the time of our review, the company employed a relatively streamlined, mainly qualitative methodology to assess information security risk. A headquarters-level risk management coordinator, responsible for security risk assessments, was the focal point for the risk assessment program. The methodology followed defined steps for analyzing potentially damaging scenarios and involved a number of standardized tools, including software developed in-house, to compile and analyze data and generate reports. Each assessment consisted of three phases--planning and preparation, team risk assessment activities, and report development. These phases generally took a total of 2 to 4 weeks to complete. Additional time was required for the business unit to develop an action plan for responding to recommendations resulting from the risk assessment.

The key steps of the process are shown in the following diagram and discussed in greater detail on subsequent pages.

**Figure 3: Risk Assessment Process Diagram #1**



## **Initiating a Risk Assessment**

The organization's policy guidelines require that risk assessments be performed prior to any significant change in a facility or operation, after a serious security incident, or whenever a new significant risk factor is identified. Regardless of these considerations, the organization's objective is to assess or reassess risk of all critical operations at least every 3 years.

Company guidelines direct the manager of a project, facility, or segment of operations to notify his or her respective regional security coordinator of the need for a risk assessment. Notification is usually in writing. The regional coordinator then notifies the organization's central security risk management coordinator in writing of the upcoming assessment. Business units are mindful of the need and significance of conducting risk assessments due largely to the strong support given by the organization's senior executives. Although the business manager is primarily responsible for initiating risk assessments, the central coordinator routinely reviews internal budget and project documents to identify operational segments that may require a risk assessment.

## **Conducting and Documenting the Assessment**

The risk assessment process can be divided into three distinct areas: planning and preparation, team risk assessment activities, and report development.

### **Planning and Preparation**

After notification of an upcoming risk assessment, the central coordinator, in conjunction with senior managers in the business unit, develops a risk assessment execution plan. This plan covers assessment objectives and methodology, team size and composition, and information requirements for conducting the assessment. Developing the plan is an iterative process between the central coordinator and business unit management. According to the central coordinator, the final plan must receive business unit management endorsement.

The risk assessment team is multidisciplined, usually consisting of about five to eight individuals with specialized knowledge of the business unit's assets and operations. Team members are usually employees; however, on occasion, the team includes outside consultants. Senior managers of the business unit select the team with approval from either the regional or central coordinator. To help ensure objectivity, the risk assessment team leader is selected from outside the unit being assessed. In addition, security specialists from the business unit in question are usually not part of the risk assessment team; however, they are interviewed to obtain information on security issues.

Individuals, primarily from the business unit, are the main source of data on all aspects of business operations and assets. For this reason, identifying knowledgeable individuals



to be interviewed and developing interview questions are critical parts of the planning process that require careful attention and close coordination between the business unit manager and the regional and central coordinators. A wide array of individuals ranging from senior managers to security specialists and contractors are interviewed. Organizational guidance states that midlevel managers from key business units are to be interviewed, including individuals with knowledge of legal, safety, personnel, and operations matters, as well as related processes.

The list of interview questions covers many areas of information security, including information classification; information storage, handling, destruction, and disposal; access controls; and transmittal of mail, data, fax, video, and voice.

To help ensure that all credible threats are considered, this company has established a separate corporate group that develops and maintains threat data for use by the entire company, including risk assessment teams. This group collects threat data from internal and external sources, including federal intelligence agencies and emergency response centers, such as those at Carnegie Mellon University and Lawrence Livermore National Laboratory. Based on this information, the group develops a "baseline threat statement" that identifies the possible threats from outsiders, insiders (trusted employees and support personnel), and system-induced events (faulty processes). At the time of our study, the baseline threat statement in use was four pages long.

The central coordinator told us that the costs of risk assessments are divided between the corporate security office and the business unit. The corporate security office pays the central coordinator's salary and travel costs. The coordinator's travel costs are often the main concern, since the organization has many overseas operations, and assessments are generally conducted in the field. Most team members are employed by the business unit being assessed, so the cost of their time is covered by that unit.

Prior to convening, the central coordinator provides each team member a 10- to 15-page package of information that includes a copy of the agreed upon execution plan, an assessment schedule, a copy of any previous risk assessment reports for the system or facility being assessed, threat data, a summary describing the risk assessment methodology, and a list of suggested interview questions. Because of his familiarity with the tools and the reporting requirements, the coordinator helps reduce the amount of training required for team members.

### **Team Risk Assessment Activities**

The primary focus of this phase is collecting and analyzing data on threats and potential vulnerabilities and recommending corrective actions to reduce or mitigate risks. This phase usually takes about 5 days to complete—3 days for data collection and another 2 days for data analysis.

The first steps in this segment of the process are conducting interviews with the knowledgeable individuals identified during the planning stage and reviewing related documentation. Depending on the scope, the team conducts 20 to 40 separate interviews lasting about 1 hour each. To maintain objectivity, team members usually do not interview superiors or co-workers. Although the first 3 days are targeted toward conducting interviews, the team convenes at the end of each day to start analyzing the information collected during the interviews and to develop scenarios of possible undesired and damaging events. In a typical information security risk assessment, 10 to 20 scenarios are developed.

In developing scenarios, risk assessment teams consider how current organizational policies or procedures may compromise the organization's information resources and ultimately damage the company. Considerations include disclosure of information to unauthorized individuals and organizations, loss of information, and inability to access company information due to computer malfunction or loss of communications. As part of this, the team considers the baseline threat statement, to which specific local threat data have been added.

A scenario developed as part of a recent assessment was of an employee with personal financial problems, unknown to corporate managers, who might independently access highly sensitive and confidential information on company operations and sell such information to outsiders. In this case, the threat was an employee with a strong incentive to misuse or disclose company assets for personal gain. The asset at risk was proprietary information of great value to the company.

Once the scenarios are complete, the team ranks them according to how severe the effects of their damage or loss would be. To assist in this process, the company has adopted and modified categories originally developed by the Department of Defense to categorize damage and/or loss, as follows.

- Category I    Death, loss of critical proprietary information, system disruption, or severe environmental damage
- Category II    Severe injury, loss of proprietary information, severe occupational illness, or major system or environmental damage
- Category III    Minor injury, minor occupational illness, or minor system or environmental damage
- Category IV    Less than minor injury, occupational illness, or less than minor system or environmental damage

The team then ranks the probability of scenarios materializing. The following categories are used for this ranking.





Category A	Frequent - Possibility of repeated incidents
Category B	Probable - Possibility of isolated incidents
Category C	Occasional - Possibility of occurring sometime
Category D	Remote - Not likely to occur
Category E	Improbable - Practically impossible

For the scenario previously cited involving a company employee selling proprietary data, the team concluded—after consideration of existing controls and a scenario cause-effect analysis—that such an event was probable (category B), in part because background investigations for employees with access to highly sensitive information were not updated frequently.

After severity and probability levels are determined for each scenario, the team compares them to a predetermined set of four categories that describe the company's policy on (1) which risks are considered unacceptable and which are of less significance and (2) the need for corrective action. Figure 4 illustrates the matrix that the company uses to perform this analysis. The accompanying category descriptions define the severity levels and required action.

**Figure 4: Risk Assessment Matrix**

Severity Level	Probability of Occurrence				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I (High)	Very High Risk	High Risk	Medium Risk	Low Risk	Very Low Risk
II				Medium Risk	
III		Low Risk	Medium Risk	Low Risk	
IV (Low)	Very Low Risk	Low Risk	Very Low Risk	Very Low Risk	

-  = Risk 1 (undesirable and requires immediate corrective action)
-  = Risk 2 (undesirable and requires corrective action, but some management discretion allowed)
-  = Risk 3 (acceptable with review by management)
-  = Risk 4 (acceptable without review)

The above steps are facilitated by the use of an internally developed software program, which captures information on scenarios. The software proposes corrective actions based on a list of security controls built into the software and provides a related cost estimate. According to the central coordinator, the software allows for real time, cost-benefit analysis of security investments.

For each scenario requiring risk reduction, the team identifies one or more possible corrective actions from a list of suggested corrective actions predetermined by the organization. The organization has established guidance on suggested types of corrective actions for each of the four risk categories.

The team selects for recommendation the most appropriate corrective actions based on (1) the effectiveness of the control in reducing either the probability or severity of a potential scenario and (2) cost. To illustrate the effect of the recommended corrective actions, the risk assessment team recalculates the new level of risk that would exist if the corrective actions were implemented.

## Reporting and Ensuring that Agreed Upon Actions are Taken

After the team develops and recommends corrective actions, it prepares an exit briefing to discuss the assessment findings with the business unit's management. This briefing usually takes about 45 minutes. The team will highlight high-risk scenarios—some of which may require immediate action. After the briefing, the team disbands. The central coordinator then prepares a draft report, using a standard format, and distributes the report to team members for comment. To ensure objectivity, each team member

independently reviews the draft. The team leader considers team input, finalizes the report, and provides it to the business owner. The team may provide the report to others in the organization depending on the issues involved.

Within 2 months of receiving the risk assessment report, the business unit is to develop an action plan for implementing the report recommendations. In the event that the business unit decides not to implement a recommendation associated with higher risk scenarios, its managers must document their justification and suggest an alternative solution for reducing the risk. If the scenario has the potential for affecting other organizations, the central coordinator meets with the unit manager to discuss and approve the alternative solution. Corporate management does not need to approve the business owner's alternative solution if the impact is limited to the unit in question, or if the risk is at either level 3 or 4. The action plan for addressing recommendations and/or new alternatives is to identify actions planned, resource requirements, responsible personnel for each action, and a schedule for anticipated completion dates. Senior business unit managers document approval of the plan in writing and send copies to both the central and regional coordinators.

The central and regional coordinators monitor the status of each recommendation until the recommendation is fully implemented. The central coordinator maintains records on open recommendations and issues quarterly status reports. Once a recommendation is closed, the business owner prepares a closeout report and submits it to the central and regional coordinators. Regional coordinators are also responsible for ensuring that recommendations are implemented and that periodic updates and verification occur, usually annually.

## **Case Study 2: Financial Services Company**

### **Distinguishing Characteristics**

- Used annual risk management plans as a basis for determining when risk assessments were needed.
- Held central focal point group meetings to discuss crosscutting risk issues.
- Established formal process for documenting acceptance of risk.

This is an established institution that handles relatively large-dollar transactions and considers itself to be conservative and risk averse. It views the protection of the integrity, confidentiality, and availability of its information assets and networks as a strategic objective. Although the organization has been performing information security risk assessments for 15 years, the information risk management program has become more robust and formalized in recent years. The fundamental basis of the risk assessment program is to balance the company's security requirements with other factors associated with doing business. The company recognizes that some risk must be accepted to conduct business.

The program provides a practical, realistic approach to efficiently and cost-effectively identify risks associated with the organization's information systems. The company's assessment process helps ensure that business unit managers comply with mandatory corporatewide security requirements and make informed decisions about the need for additional risk-reduction measures. The process also raises the awareness of business managers regarding the risks associated with their business unit's reliance on automated systems and electronic information. The process does not focus on identifying specific threats, but rather on protecting the organization's information regardless of the threats.

Key steps of the process are shown in the following diagram and discussed in more detail on subsequent pages.

```

graph TD
    Start([Start]) --> Step1[Select system & prepare for assessment]
    Step1 --> Step2[Hold meetings to rank information criticality and identify existing controls]
    Step2 --> Step3[Compare existing controls with mandatory and optional control requirements]
    Step3 --> Dec1{Are there gaps?}
    Dec1 -- No --> Step4[Document & disseminate results]
    Dec1 -- Yes --> Step5[Recommend solutions to correct gaps]
    Step5 --> Step3
    Step4 --> Step6[Develop risk acceptance statement]
    Step6 --> Doc1[Risk acceptance statement]
    Doc1 --> Step7[Develop risk acceptance statement]
    Step7 --> End([End])
  
```

**Legend:**

- Process (Rectangle)
- Individuals Involved (Shaded Rectangle)
- Where results reported (Parallelogram)
- Decision (Diamond)
- Document (Wavy-bottom Rectangle)

## **Initiating a Risk Assessment**

Business units initiate risk assessments based on each unit's annually updated risk management plan. To develop a risk management plan, a variety of information sources are used, including prior risk plans and assessments, business plans, audit reports, and the expertise of other business and technical managers. The need for a risk assessment is based on a system's criticality to business operations, the sensitivity of its information, and the lapse of time and type of changes since the last assessment. Generally, risk assessments are performed on critical information systems about once a year.

In the risk management planning process, business managers are asked to identify, based on their knowledge of the business unit's operations, the most important systems to their business units. Some business units have as few as five critical systems, while others have as many as 130 critical systems. Based on this list, business units focus their risk assessment activities on the top 10 to 20 critical systems. According to one official, performing risk assessments for more than 10 to 20 applications would become overwhelming, cumbersome, and strain limited resources. After the systems are selected, the business managers classify the systems' information as being high, medium, or low risk.

Next, the list of required assessments is further narrowed to the most critical systems with the highest risk. The risk assessment process for existing systems focuses on existing risks associated with the security of the system being assessed. For new applications, the unit attempts to build security into the systems as they are developed so that security is a part of a system's design from the start.

## **Conducting and Documenting the Assessment**

The company has a standardized risk assessment process; however, individual business units have some latitude in how assessments are conducted. Each business unit head designates an individual, directly under him or her, with continuing responsibility for facilitating, coordinating, and executing the business unit's risk assessment activities. Throughout the risk assessment process, this focal point receives assistance from employees with expertise in business operations and processes, information resource management, systems use, and risk factors affecting multiple business units. In addition, the organization's information technology staff assists the focal point, as well as the business unit's head, in understanding existing technical controls and developing solutions to identified security weakness.

The time and effort taken to complete an individual assessment varies from 1 to 2 days to several weeks, depending on the size and complexity of the system being assessed. The system's use across multiple business units also affects the time it takes to complete an individual assessment. Typically, the focal point dedicates the equivalent of one full



day's work to an individual assessment, while each of the participants dedicates no more than the equivalent of 1 week of work.

### **Select System and Prepare for Assessment**

Once a system is selected from those identified in a unit's risk management plan, the focal point collects preliminary information from the business unit's managers and from documents, such as project initiation and definition reports, audit reports, and functional specifications. The focal point also determines the changes made to the system since the last assessment and identifies from the documentation the technical components of the system. In addition, qualitative aspects of the system are documented, including a brief description of the system's purpose, functionality, and location; the system's user authentication procedures; and the procedures for establishing new user accounts and access privileges.

### **Hold Meetings to Rank Information Criticality and Identify Existing Controls**

After gathering preliminary information, the focal point schedules a meeting to reach a consensus regarding the level of risk associated with the selected system and identify the existing technical controls and manual processes to mitigate system risks. Generally, the focal point selects individuals from the business unit to participate in the meeting who have expertise in business operations and processes, information resource management, information technology, and system use. The focal point also includes employees with knowledge from outside the business unit that may affect information security risk, such as information on political and economic conditions in specific geographic regions.

Prior to the meeting, the focal point sends the participants a standardized questionnaire so that they have an opportunity to informally consider the system's characteristics in comparison to the company's control requirements. The questionnaire serves as a tool for documenting the selected system's compliance or noncompliance with specific control techniques established in the company's security standards for operating systems, networks, data stores, and applications. The questionnaire organizes specific control techniques under nine control elements--authentication, access control, environmental integrity, information integrity, confidentiality, availability, audit, nonrepudiation, and administration. The control techniques are further divided into either mandatory or optional requirements. The mandatory requirements are the minimum set of information security controls that is required for all operations and represent the organization's "target information security environment." The optional requirements are additional security controls that may be required for certain higher risk operations. These risk levels and the classification of the system's information are factors established during the risk

management planning step. The optional requirements provide greater control over systems or information that is especially important to the business unit or perceived to be at especially high risk. An abbreviated example of the questionnaire follows.

**Figure 6: Abbreviated Example of Standardized Questionnaire**

Control elements	Standards							
	Operating system		Network		Data store		Application	
	Complies	Discuss	Complies	Discuss	Complies	Discuss	Complies	Discuss
<b>1. Authentication</b>								
-- The identity of all users currently logged onto the system must be internally maintained	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-- All data passed through the network must identify the originator and recipient			<input type="checkbox"/>	<input type="checkbox"/>				
<b>2. Access control</b>								
-- Only authorized authenticated users and remote applications may have access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
-- Network access must be based on a business requirement			<input type="checkbox"/>	<input type="checkbox"/>				
Legend: <input type="checkbox"/> Mandatory <input type="checkbox"/> Optional								

During the meeting, the focal point and the other participants use the questionnaire as a guide for their discussions and as a tool for formally documenting the decisions made. Additional manual tools are available to assist the participants in evaluating (1) the system's information risk levels for both sensitivity and criticality, based on a simple low, medium, or high ranking for each system and (2) the inherent vulnerabilities of the target operating environment, based on a numeric system. By combining the results of

these evaluations, the participants determine the level of threat to the system. According to one organization official, any greater refinement of the analysis is not valuable.

The focal point documents the decisions made during the meeting. Most of this documentation is subsequently maintained in a database, where it is available to other business units. Although use of the database varies across the business units, it is especially valuable for providing information on assessments done on systems used by multiple business units.

In addition, the focal point determines and documents the system's minimum-security requirements based on the final results of the questionnaire and the level of threat to the system established during the meeting. The focal point's decisions are not formally approved by anyone, but they are summarized in quarterly reports that also describe the status of the systems in their business units using a simple red, yellow, and green scheme to show the level of risk to the system. The company's chief information risk officer and his staff carefully review these scorecards and ask for justification regarding questionable decisions.

A risk assessment is stopped at this point if it is discovered that the system being assessed has low criticality and sensitivity. Typically, the only time that a low-risk system would be assessed is when external connectivity is an issue, for example, if a business unit wanted to provide network access to a third-party vendor.

### **Compare Controls with Mandatory and Optional Requirements to Identify Security Exposures**

During this step, the focal point analyzes the system's compliance with the minimum-security requirements, as established in the previous step, and determines the acceptable level of risk exposure for the system. When unacceptable exposures are found because there is a difference between the system's minimum-security requirements and the controls in place, there are two possible courses of action. First, if there are solutions or compensating controls that are feasible and can be implemented in a reasonable time, then the focal point can develop preliminary recommendations for addressing those exposures. Otherwise, the business unit manager must accept the risk exposure and a risk acceptance statement is created, as discussed later. During this step, the information technology staff and system users are consulted to assist in the identification of security solutions and recommendations.

### **Recommend Solutions to Mitigate Exposures**

If feasible solutions or compensating controls exist for the information security exposure(s) identified in the previous step, the focal point and the business unit's information manager develop an action plan that documents the business unit's

recommendations to mitigate the exposure by implementing new or strengthened controls. The action plan includes the steps to be taken, the time frame for completion, and the responsible groups within the business unit. The length of the action plan varies, though according to one focal point, the plan should be concise and focus on a few key recommendations. The business unit head makes the final decision in regard to what actions are taken to correct the exposure(s) and is responsible for executing those actions. After the recommendations have been implemented, the focal point initiates another analysis to ensure that the controls have been properly implemented and the exposure no longer exists or the risk has been reduced.

### **Develop Risk Acceptance Statement for Remaining Exposures**

If the security solution or compensating control in regard to the identified exposure(s) is not feasible or can not be implemented promptly, the business unit head is informed about the exposure and its potential impact on the business unit's operations. If the risk exposure is exclusively related to the business unit's systems or operation, then the business unit head is responsible for deciding if the risk should be accepted. If the risk exposure affects multiple business units or the corporation's overall network, the responsibility for the accepting the risk escalates to higher management levels, typically the chief information officer, for a decision.

If the responsible manager is willing to accept the risk, a risk acceptance statement is prepared that explains why an exception to a mandatory or appropriate optional requirement is necessary. In addition, the statement includes details about the risk and exposure, compensating controls to be put in place, loss potential, expiration date of the exception, and review procedures. To ensure accountability, the statement is generally prepared by the focal point and signed by the business unit head or equivalent. Typically, risk acceptance statements are required for all instances of noncompliance with standards that represent material risks to the systems. Areas that are low risk and common vulnerabilities that are generally known to exist typically do not require a risk acceptance statement. If the business unit head is unwilling to accept the risk, recommendations to reduce or eliminate the exposure(s) are developed, as discussed previously.

### **Approve the Risk Acceptance Statement**

After the risk acceptance statement is completed and signed by the responsible manager, it is submitted for review and approval to the corporate information risk group, global information risk coordinator, relevant audit staff, and other interested parties. In cases where the accepted risks could impact the corporate network, a committee made up of representatives from all of the business units also reviews the statement.

The corporate information risk group grants the exception to the security requirement if there is concurrence by all of the reviewing parties that there would be no detrimental affect on the other business units. If it is determined that an exception will affect other business units, the request is escalated to higher management levels, typically to the chief information officer, for approval. Generally, a consensus is reached that accommodates the exception, but entails additional compensating controls to reduce the exposure.

An approved exception is typically good for 6 to 12 months, depending on the circumstance. When the exception expires, the decision is re-evaluated by the corporate information risk group. During the re-evaluation, the group determines if the exposure still exists, what progress has been made to mitigate the exposure, and if the acceptance of the exposure is still appropriate. If the group decides that acceptance of the exposure is still appropriate, the exception is extended. If not, the business unit's manager and focal point must develop means to eliminate or further mitigate the exposure.

## **Document Results**

All information risk assessments are documented in a database, as previously mentioned. Even when no corrective actions are needed, the documentation may be useful in subsequent analyses and as input for future risk management plans and risk assessments. Paper copies of the risk acceptance statements are maintained so that the chief information risk officer's staff can monitor expiration dates and related actions underway by business units.

Additional documentation that is provided to corporate-level and business unit management consists of risk assessment reports, the status of summary databases, and the business unit's external connectivity status. The internal auditors also use the documentation to review the decisions made by the focal points and other participants during the risk assessment process. According to one official, the internal audit reviews provide a valuable service regarding the quality of the risk management decision-making process.

## Case Study 3: Regulatory Organization

### Distinguishing Characteristics

- Emphasized exploring and ranking risk to business operations.
- Applied a predefined set of minimum control requirements for each of three risk levels (high, medium, low).

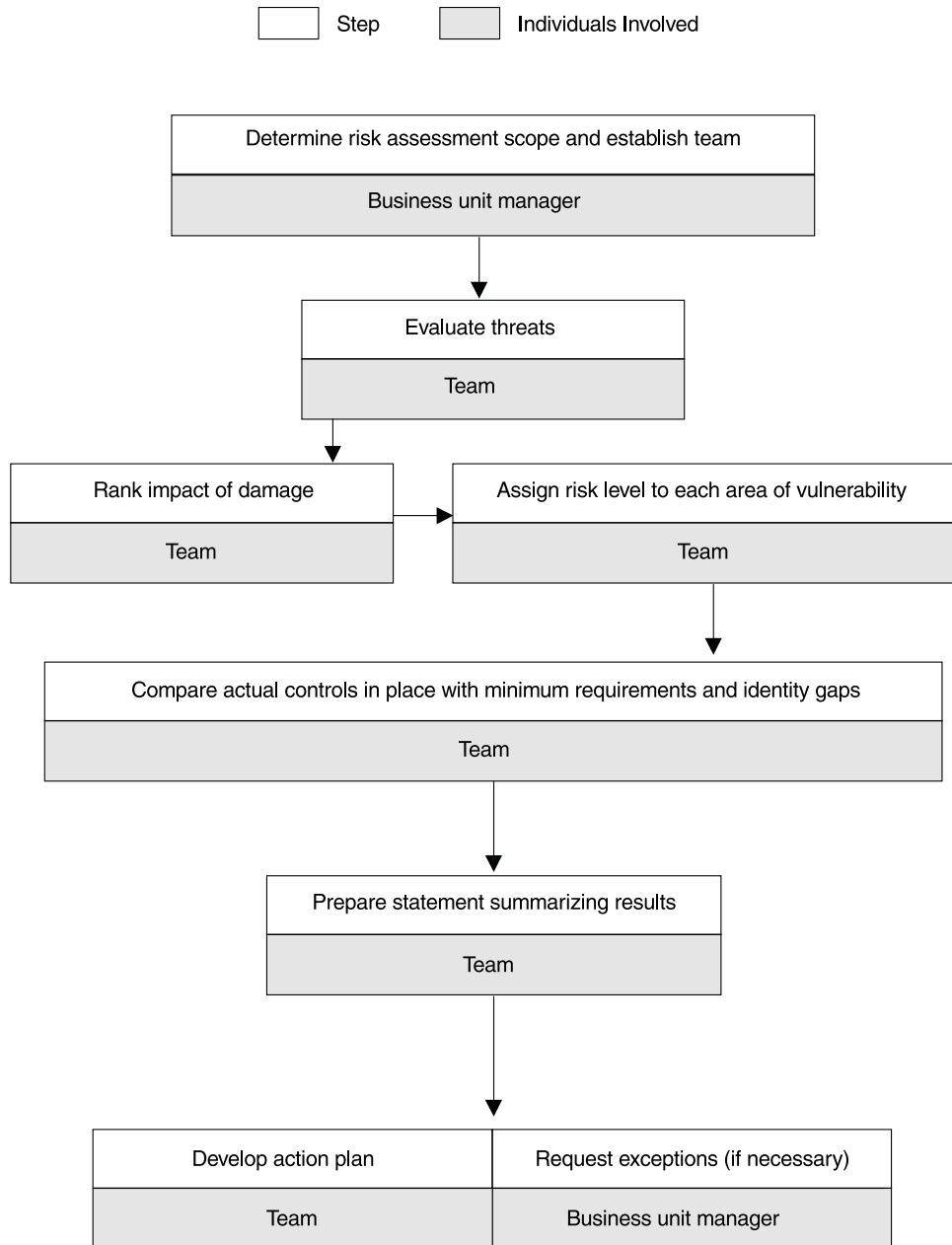
This organization considers itself to be risk averse and is particularly concerned with loss of customer confidence, as well as monetary and productivity losses. As such, the organization has developed a detailed set of minimum mandatory control requirements over all operations.

Although risk assessments have always been a part of doing business, the organization implemented a more standardized approach in 1995 to ensure a more common understanding and to provide a systematic approach that reduces the risk of overlooking issues. The objective of the risk assessment is to determine the level of risk associated with a business function or process in order to determine the applicable security controls. This is done by determining which of a predefined set of controls is appropriate for individual business operations and comparing what is appropriate to controls already in place in order to identify and address gaps.

The organization consists of a central office and regional offices throughout the United States, with each unit having its own area of responsibility for the assessment. The central office issues organizationwide information security risk assessment guidelines and establishes minimum control requirements; the regional office oversees and facilitates the process in its geographic area; and individual business units are responsible for conducting the assessments.

The key steps of the process are shown on the following diagram and discussed in greater detail on subsequent pages.

**Figure 7: Risk Assessment Process Diagram #3**



## **Initiating a Risk Assessment**

The organization's policy guidelines require business units to conduct risk assessments at least once a year. Assessments are also required when a new business operation is established or when significant operational changes occur. Responsibility for initiating the assessment lies with the business unit manager. The regional audit department reviews compliance with the organization's risk assessment requirements through annual audits and reports any noncompliance to business unit management.

After identifying the need for a risk assessment, the business unit manager determines the scope of the assessment and establishes a risk assessment team. The assessment can cover an entire unit or a specific segment of operations depending on how information is accessed, processed, or disseminated. The assessment team usually comprises five to seven individuals with expert knowledge of the business unit's assets and operations, and members from the region's information security office and audit department. After the team convenes, a representative from the region's information security office briefs team members on the risk assessment process and provides them with organizational guidance on conducting assessments.

## **Conducting and Documenting the Assessment**

Risk assessment teams use predefined categories—developed by the central office—for ranking risk assessments. The categories cover specific elements that must be addressed for each assessment. These elements include five areas of potential vulnerabilities, four types of damage, and three possible consequences, as shown in the following diagram. The purpose of predefined categories is to ensure a consistent approach throughout the organization.



## Figure 8: Elements Considered in Ranking Risk

### Areas of vulnerability

- Personnel
- Facilities and equipment
- Applications
- Communications
- Software and operating systems

### Types of damage

- Unauthorized disclosure, modification, or destruction of information
- Inadvertent modification or destruction of information
- Nondelivery or misdelivery of service
- Denial or degradation of service

### Potential consequences

- Monetary loss
- Productivity loss
- Loss of customer confidence

The central office has incorporated these elements into a set of detailed guidelines for conducting information security risk assessments. The office has also prepared a complementary training manual elaborating on the guidelines and providing more detailed step-by-step procedures.

## Determining Risk Level

The team's first step is to evaluate possible threats to information security that may affect the unit's operations and, based on its knowledge of the operation being assessed, consider the likelihood and consequences of the threat occurring.

The team assigns a risk level of high, moderate, or low for each area of vulnerability to show the possible effect of damage if the threat were to occur. In completing this step, the risk assessment team assumes that **no controls** are in place. (Later in the assessment, existing controls are compared to a comprehensive set of control requirements to identify shortfalls.) The team uses a matrix to assist in its analysis of risk as shown in the following table:



**Table 1: Risk Assessment Matrix**

Areas of vulnerability and possible effects of damage	Risk of monetary loss			Risk of productivity loss			Risk of loss of customer confidence		
	H	M	L	H	M	L	H	M	L
<b>Personnel</b>									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
<b>Facilities and equipment</b>									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
<b>Applications</b>									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
<b>Communications</b>									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
<b>Software and operating systems</b>									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									

After completing the matrix, the team summarizes its findings by assigning a composite risk level to each of the five areas of vulnerability on the matrix. The team does this by considering the four potential types of damage identified under each area of vulnerability and judgmentally assigning a risk level of high, medium, or low to each area. The team then agrees on an overall risk level for each vulnerability in the last column of the table marked "Overall risk." Table 2 is used to record this step.

<b>Table 2: Risk Assessment Table</b>				
	<b>Risk category</b>			
<b>Areas of vulnerability</b>	<b>Monetary loss</b>	<b>Productivity loss</b>	<b>Loss of customer confidence</b>	<b>Overall risk</b>
Personnel				
Facilities and equipment				
Applications				
Communications				
Software and operating systems				

### Identifying Needed Controls Based on Predetermined Requirements

After determining the overall risk level for each area of vulnerability, the team identifies the minimum applicable controls that are prescribed in its organizational guidelines. The guidelines describe minimum requirements for each of three levels of risk—high, medium, and low. Guidelines require that each higher risk category incorporate the controls of lower risk categories. For example, a “high” risk level incorporates controls from each of the three levels of risk—high, medium, and low. Similarly, “medium” risk includes controls for both medium and low risk levels.

## **Reporting and Ensuring that Agreed Upon Actions are Taken**

After determining the minimum set of controls, the team compares those required controls with controls already in place and identifies any gaps. The team prepares a short statement summarizing the outcome and documenting its decisions and decision-making process. It then provides the regional office a copy of the risk assessment table. Guidelines require the business unit being assessed to retain the completed matrix and documentation supporting the outcome, such as major threats considered, and major decision points, such as the team's rationale used in arriving at the appropriate level of risk.

If there are areas where additional controls are needed to meet minimum requirements, the business unit manager develops an action plan and submits it to the regional office. The plan includes those controls the business unit manager believes would provide the level of protection appropriate for the risk associated with the asset. Factors considered are security exposures, the level of risk associated with the business function or activity, the costs of implementing the controls, and the impact of noncompliance on other business units or operations within the organization.

If the business unit believes that the time needed to implement controls is too lengthy or the steps required are too costly, the business unit manager may request a waiver. The business unit manager must describe the rationale for the waiver and what compensating controls the unit has or will implement. The regional office has a standing committee to approve or deny requests for waivers; however, the central office must approve or deny requests that may impact the entire organization or multiple regional offices. If a waiver is approved, it is usually approved for a period not to exceed 1 year.

In early 1997, the regional information security office began using an internally developed software program to monitor compliance with applicable policies and safeguards. Regional officials said that use of this program facilitates preparing reports to high-level officials and provides easy access to individuals with a need to know. The tracking system contains information on the regional office's business units, such as operations descriptions, risk assessment results, and associated policy and safeguard compliance. The system keeps this information in a central database with distributed access to business unit personnel responsible for ensuring compliance and to the regional security office.

## **Case Study 4: Computer Hardware and Software Company**

### **Distinguishing Characteristics**

- Used expert system to analyze data and develop recommendations.
- Conducted extensive quality review of data.
- Included risk assessment as part of employee performance expectations.

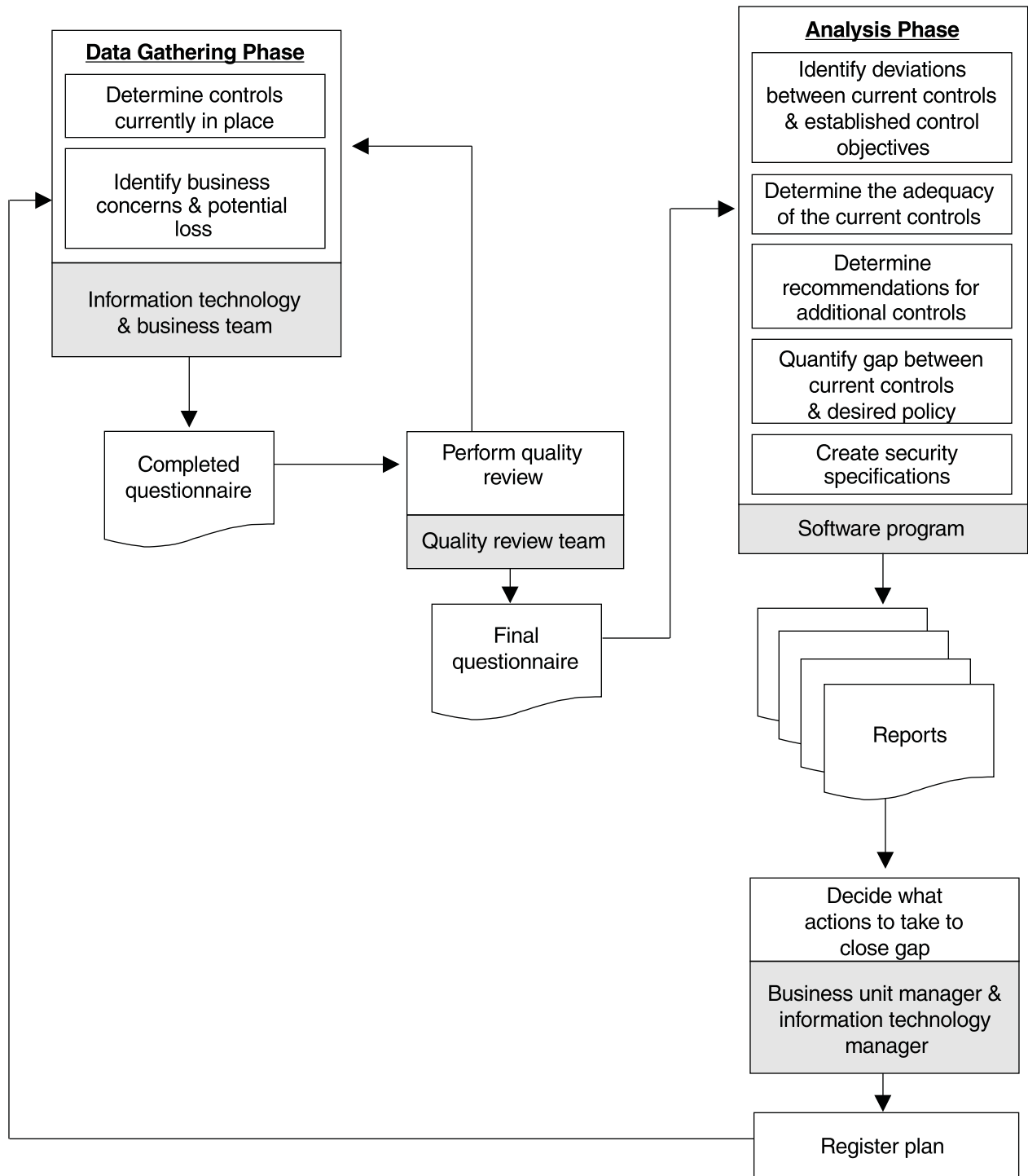
This organization uses a defined risk assessment process to ensure that information security controls in place comply with established requirements. The risk assessment process was initiated due to the company's efforts to pursue more secure electronic commerce and increased integration of information systems within the company and with its customers, suppliers, and stockholders. Using a combination of qualitative and quantitative methods, the process is designed to take advantage of the company's expert knowledge of its applications and related security requirements, scale results in such a way as to minimize unreasonable recommendations, and establish the minimum adequate amount of security across the company. The execution of the process identifies and documents the current security controls in place for the operations under assessment, identifies the current risks to the systems, and identifies additional controls needed to provide an appropriate level of risk mitigation.

As a hardware/software company, the organization provides its customers with network hardware and software, support services, and consulting services. The company conducts business in over 110 countries and operates its network in over 68 of those countries. It uses thousands of systems to execute the day-to-day functions of the company, including numerous network connections to customers, suppliers, and partners. Protecting the information resources that support these operations is especially challenging at this company because its engineering culture thrives on openness and sharing of data.

The key steps of the process are shown in the following diagram and discussed in greater detail in subsequent pages.

**Figure 9: Risk Assessment Process Diagram #4**

□ Step    ■ Individuals Involved



## **Initiating a Risk Assessment**

At this company, organizational policy requires the corporate information security group to initiate risk assessments based on the importance of the operations and the time lapse from the last assessment. Business unit managers assist in determining what the most important operations are within their business units. The general expectation is that risk assessments are to be performed on important operations annually. In instances where the operation is extremely critical or has changed significantly, risk assessments could be performed more often. In addition, at any time, business unit managers can request that a risk assessment be performed.

The risk assessments are associated with three types of activity—(1) development of new computer systems, (2) procurement of production systems from other vendors, or (3) improvement of legacy system security features—and, generally, are limited in scope to a primary business process and supporting systems. The supporting systems include the software, databases, and the hardware and network technology supporting the software, as well as the people who use and rely on these resources. Business unit managers are responsible for executing the risk assessments associated with their unit's computer-based operations, and such responsibilities are generally documented in their performance expectations.

Once a decision is made to perform a risk assessment, the business unit manager forms a team of information technology and business experts to conduct the first part of the assessment, which entails collecting data. The size of the team depends on the number of business and technical people involved in the operation being assessed. Often 12 to 14 people are part of the team, but the number can vary. In addition, the organization uses a cadre of other individuals to perform risk assessment tasks, including performing quality reviews, analyzing the results using a software tool, and facilitating the process across the organization.

## **Conducting and Documenting the Assessment**

The organization's risk assessment process involves (1) using a questionnaire to compile information on the value of critical operations and assets, policies and controls in place, and other system attributes and (2) comparing this information with predetermined policy and control requirements. The company has developed a software program that automatically performs this comparison. When the analysis identifies an area that does not meet the established control requirements, the software program automatically accesses a database of suggested control solutions that has been developed by company experts. These control solutions form the basis of recommendations generated by the analysis.



## Data Gathering Phase

During this phase, the team completes a questionnaire, developed by the organization for the risk assessment process, to determine what controls are currently in place over the operations being assessed. An individual experienced in applying the questionnaire assists the team and helps ensure greater quality and consistency of the answers and greater certainty that the team members provide accurate answers.

At the time of our study, the questionnaire, which is continually subject to change, had 260 multiple choice questions divided into the following categories:

- valuation of the operation,
- policy implementation,
- training,
- authorization process,
- authentication process,
- identification process,
- disaster recovery,
- physical security,
- confidentiality/integrity/nonrepudiation,
- audit,
- detection,
- incident response,
- configuration criteria,
- configuration management, and
- graphical inventory of the systems architecture

The multiple choice questions have been designed to precisely capture a description of existing operations and controls. Examples of the types of questions included are shown in the following box.

### Figure 10: Questionnaire Items Related to Authorization

1. Estimate the percentage of user population accessing this application regularly from the following sites. From those sites with access, enter the percentage value for the appropriate site. (Total of all answers may exceed 100%.)
  - a. from primary organization campuses,
  - b. from private homes,
  - c. from kiosks,
  - d. from contractor, partner, or supplier sites with whom there is a written contract to manage info-security,
  - e. from customer sites,
  - f. from sites with nomadic accounts,
  - g. from executive suites,
  - h. from anywhere,
  - i. from contractor, partner, or supplier site without info-security contract, and/or
  - j. unknown.
2. Estimate the number of administrators and other key staff listed below for this application system. [Comment: The purpose of this question is to determine the number of people who are in key positions to effect the security of the system. Please be sure to count the number of staff associated with this application from all organizations involved.]
  - a. database administrators,
  - b. application administrators,
  - c. system administrators,
  - d. access control and account administrators,
  - e. technical support operations,
  - f. security administrators or coordinators,
  - g. IT developers, and/or
  - h. unknown.

The company treats the “valuation of the operation” section of the questionnaire as a separate phase of the risk assessment. During this phase, the team determines (1) what consequences need to be protected against, assuming an attack or other damaging event occurs and (2) what the likely damage to the company would be as a result of such events. Because these valuations are considered very subjective, the team relies on the assistance of additional experts with specific finance related knowledge, who are typically from the company controller’s office. The information developed during this phase is critical to determining the significance of any control deficiencies that may be identified later in the analysis.

The team first determines what consequences could occur. The company has defined potential damage as including fraud, operational outage, embezzlement, extortion, theft of intellectual properties, regulatory violations, or diminishment of the organization's

image. Although the questionnaire is intended to be comprehensive, the company recognizes that additional types of damage may need to be considered.

Once it is determined what consequences apply to the operations under assessment, the team estimates the level of damage that could result from these consequences by considering the potential costs of restoration and recovery, as well as secondary effects, such as embarrassment and loss of credibility. Estimating the cost of secondary effects is especially difficult because of the uncertainty associated with the ultimate impact on such intangible factors. For example, the cost of restoring a damaged web site is much easier to estimate than the cost of recovering from the embarrassment and loss of credibility from such damage.

Usually, the team can complete the entire questionnaire in 1 to 2 hours. In cases where the team members are less familiar with the application, it can take up to 12 hours or more because people with additional expertise are contacted to assist in completing the questions. Once the questionnaire is completed, additional individuals perform an extensive quality review that analyzes the answers for completeness, reasonableness and consistency. Often, it takes as many as five reviews to attain the required quality. The time taken to complete the quality review varies by assessment from a few hours to several days to even weeks in rare cases. The quality review benefits the process by ensuring that (1) the data used are complete and the best available and (2) the questions are consistently applied and interpreted. Redundancy is also built into the questions to help the quality review determine if the team thoroughly considered the questions.

## **Analysis Phase**

After the quality review is completed, the analysis group inputs the information about the current controls, as derived from the questionnaire's answers, into a software program. The software program compares these controls to control requirements documented in the company's information security policies. The database of over 400 information security control requirements, which is referred to as a "policy library" by the organization, represents a consensus of the experience and best judgment of a broad group of business and information technology experts organizationwide. The analysis performed by the software identifies instances where existing controls do not meet the company's suggested control requirements.

Using the results of this comparison, additional information from the questionnaire, and a defined list of 180 control techniques, the software automatically proposes control techniques to achieve compliance with the control objectives. Each control technique, or countermeasure, can have up to five different strength levels, which generally depend on the specific type of control technique chosen and the rigor of associated enforcement efforts. Examples of strength levels for information security training are shown in the following box.

**Figure 11: Example of Five Strength Levels for Security Training**

Level 1	No specific training requirement exists, so compliance with the requirements is not measured.
Level 2	Security training requirements exist, and business unit managers record completion of the training, but compliance is not independently verified.
Level 3	Security training requirements exist, and the business unit managers determine in advance the required percentage of compliance among the individuals involved in that operation. During the periodic risk assessment, a comparison is done to assure compliance with the established percentage.
Level 4	Same as Level 3.
Level 5	Security training requirements exist, and the business unit manager is responsible for tracking and verifying that all individuals involved in the operation are compliant.

Next, the analysis group reviews and further refines the proposed recommendations using a software tool that considers a number of factors, such as the number of users, number of access paths, and effects on other systems. The organization has also designed the software tool to consider detailed requirements for individual circumstances. For example, systems with more than 150 users require more rigid account management procedures to be in place than do systems with fewer users. According to this company's policy, the attributes of these procedures for systems with over 150 users should include:

- formal procedures for revocation or modification of terminated or inactive accounts;
- centrally assigned and monitored passwords;
- a unique password for each user, with 90-day mandatory password changing; and
- screening of new passwords for suitability prior to being accepted by system.

Based on the determinations made during the analysis, the analysis group finalizes the recommendations. When necessary, systems engineers are brought into the process from the information technology area of the business unit to perform an engineering review of the assessment's output and recommendations. The purpose of this review is to determine the feasibility of the recommendations and to resolve any open issues identified, such as the need for a detailed design review. The precise technical method of implementing the recommended improvement is left to the judgment of personnel in the business unit.

## **Reporting and Ensuring Agreed Upon Actions are Taken**

A series of standardized reports are produced from the risk assessment process, including a detailed risk analysis report, a report describing the application's current level of conformance to requirements, and recommendations for specific security engineering design review. One of the key reports graphically shows, for each major application, the deviation between the current controls and the controls suggested by the company's information security policy. In addition, the reports estimate the costs for each recommended countermeasure, including costs for licenses, training, development, implementation, and recurring support.

The business unit head considers the information in these reports when deciding what new controls to implement. If the business unit head believes that certain recommendations are not cost-effective, he or she can discuss the concerns with the company's information security managers and negotiate alternative actions.

Because business and information technology managers are being held accountable for making information security improvements, the organization has developed a number of management tools to assist them. There are over 12 management reports used to gauge the organization's progress in achieving established information security goals. In addition, the organization has instituted audit and measurement procedures to ensure the effectiveness of actions taken and that these actions have not adversely affected system operations. Company officials emphasized the importance of managing the changes resulting from the information security risk assessments. They stressed that this requires instituting methods for monitoring the progress being made because changes can be expensive and managers are usually reluctant to implement them—especially when changes could adversely effect their business.

## Objectives and Methodology

The objectives of our study were to identify and describe (1) information security risk assessment methods and (2) related critical success factors that could be considered by federal agencies to improve their own processes. While recognizing that the methods described here may not be suitable for all federal operations, our study was intended to help provide ideas and options for agency officials to consider.

To identify organizations that had adopted successful methods, we solicited suggestions from a variety of sources, including the National Institute of Standards and Technology, Office of Management and Budget, private consulting firms, professional associations, a risk assessment software developer, and GAO auditors who were familiar with agency information security practices. These sources recommended over 30 private and public sector organizations that were known to have strong security programs or be actively pursuing improved risk assessment practices.

After initial discussions with a number of these organizations, we narrowed our focus to four organizations that most closely met our criteria of having implemented organizationwide information security risk assessment procedures that they considered to be practical and useful and had been in place for at least a year. The organizations selected included a multinational oil company, a regulatory organization, a financial services company, and a computer hardware and software company.

To obtain an understanding of their risk assessment procedures, we visited each of these organizations where we met with senior security officials to discuss and review the various manual and software tools they had adopted. We also obtained and reviewed each organization's written policies, procedures, and other material related to assessing information security risks. To verify our understanding of each organization's practices we conducted numerous follow-up inquiries and asked each organization to review our written summaries for accuracy. We conducted our study from April 1998 through June 1999.